Hypes and Trends in Customer Identity & Access Management (CIAM)

Andre Priebe, CTO at iC Consult

Presented during the iC Consult IAM Pit Stop Series

Pit Stop #2: CIAM

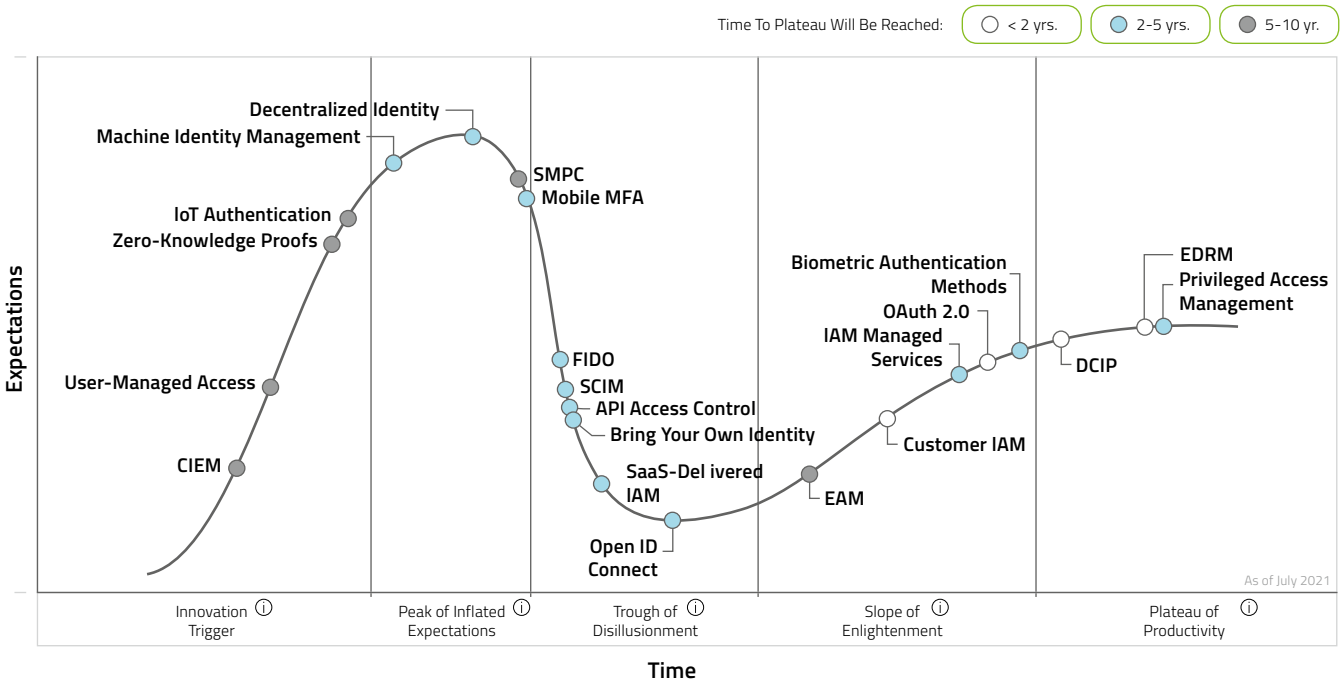
The handling of customer identities is becoming increasingly complex, and more and more organizations are implementing dedicated CIAM solutions to ensure a seamless experience, manage consent and protect critical data, and drive business in today's digital world. While CIAM is still a relatively new technology, it's also a very dynamic market, with countless exciting new capabilities looming on the horizon.

In his presentation at the second IAM Pit Stop Meeting, iC Consult's CTO Andre Priebe presented some of the most relevant trends from the recent Gartner Hype Cycle and their implications for CIAM initiatives: He discussed the potential of OAuth 2.0 and Open ID connect, looked into Document Centric Identity Proofing, and gave an intriguing outlook on Bring Your Own Identity and Password-less Authentication before wrapping up with insights into Decentralized Identity Verification. Enjoy the ride!

Content

New technologies like to make bold promises, and it's not always easy to distinguish which of the emerging trends will really end up shaping our future. A great aide for this assessment is the Gartner Hype Cycle – an annual graphic representation in which the renowned analyst lists and discusses the most important recent developments and their current maturity degree. During iC Consult's recent Pit Stop presentation, CTO Andre Priebe presented his own take on some of the upcoming identity-centric trends in the 2021 hype report.

Identity and Access Management Hype Cycle 2021



Hype 1: CIAM, OAuth 2.0 & OpenID Connect

OpenID Connect and OAuth 2.0 open the door for exciting new CIAM capabilities – but they come with some challenges.

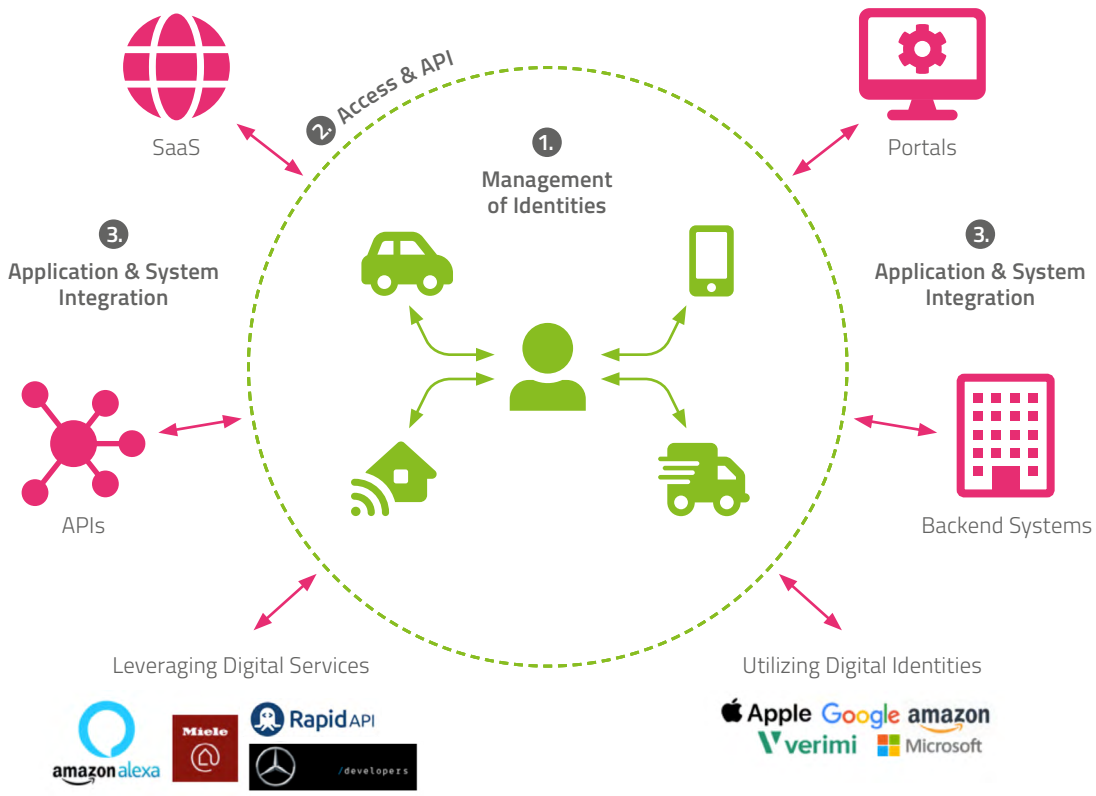
The first topic we will look at is not a single trend, but a triad of trends, which are all very closely interconnected. Let me explain why this triad might be very important for your organization first, and then we will have a look at some of the challenges you need to be aware of before implementing these technologies in your enterprise.

What is CIAM all about? It's about managing your customers' identities, and about using Customer & Identity Management as a business enabler for your organization. That said, it's not only about managing your customer's identity – CIAM is also a prerequisite if you want to market your products, and if you want to build the relation your customers have to your products. An easy example are the digital identities you need to provide access to your IT systems and your digital services. In some scenarios, identity is an add-on to your product, in others, it's needed to provide support.

But there are two more aspects we need to consider when speaking about the role of CIAM, and both are defining your interaction with the world outside your enterprise: The first aspect is how you want to leverage or integrate existing identities – for example the Apple or Google identities of your customers. I think we will all agree that these existing identities can make our life significantly easier if things are done the right way – so this is something we need to look out for. But we will address this in more depth later.

The second aspect – which is even more important in my view – is that our CIAM solutions are key to leveraging innovative digital services. A prime example is the fast-growing ecosystem of digital assistants: Sooner or later, you might decide that you want your product to be part of this growing digital ecosystem. Not necessarily because you like Amazon Alexa – but maybe simply because for a future generation of customers, Alexa will be the default way to access certain digital services. I think it's easy to see why a robust CIAM solution – and, by extension, protocols like OAuth 2.0 and OpenID Connect – are key in this kind of scenario. They will be used to define and enforce the rulesets you will have to follow if you want to be part of this particular digital ecosystem. There are several examples of this kind of ecosystem out there already. For example, some organizations are using developer portals to expose their APIs to third parties and partners, which allows the API to collect telemetry data from vehicles. This obviously paves the way for multiple exciting new business models – for example, sharing your telemetry data with your insurance company to get better premiums.

Customer Identity & Access Management as Business Enabler



And what's most exciting about it: The customers themselves get to make the decision to participate – either they allow, or they block access to their telemetry data.

The Challenges

If all of this sounds too good to be true, well, there are obviously some challenges, too. Gartner, for example, recently stressed that OpenID Connect has not fulfilled the expectations so far. So, let's have a look at the biggest issues:

Token Design
Token design is not a very complicated topic, but there are some questions your identity team will have to answer beforehand: Will you sign your tokens? Will you encrypt them? Will you use preference tokens? Which algorithm are you going to use? And how do you want to distribute the keys for encryption and signature validation? The configuration process tends to be very easy, as most CIAM solutions will guide you through it. But once you start onboarding your applications, your APIs, and your API management systems to your final solution, you will reach a point when changing the configuration becomes less and less of an option, as any changes would affect all onboarded applications. But what if you realize, after 100 or 1,000 applications and hundreds of thousands of customers, that the default token configuration wasn't quite right? By then, it will be very hard to change that! So, bear this in mind right from the start.

Authorization
In the enterprise context, authorization is typically managed via clearly defined roles. Similarly, in the new CIAM world, we have specific scopes, too – but how do these interact and how do they affect each other? Also, and that's a major point: When trying to define a robust authorization for customer identities, looking on the user perspective is not enough – you must also consider the application perspective: What is Alexa allowed to do? This is a question we need to answer as well, and you must learn to use all the tools and scopes in your box to successfully navigate these scenarios.

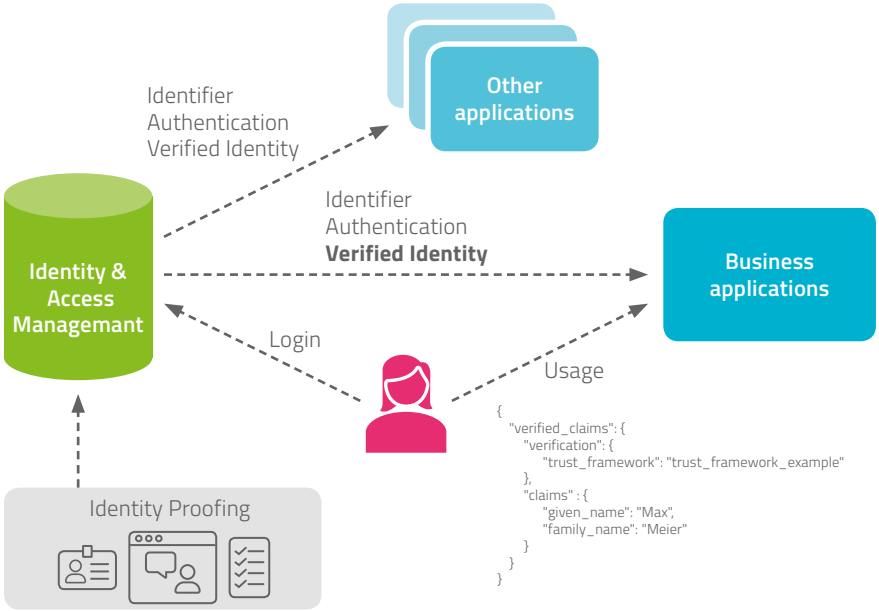
Functional Limitation
The third and final challenge is, unfortunately, functional limitations. Some very simple features like Session Termination or Log-out are not working as well as we would expect them to, based on our experience with other protocols from the enterprise world. Also, aspects like Consent Management are not as clearly defined as they should be, which is especially relevant in more complex use cases. These are known problems, and there are several new standards in the making, aimed to properly regulate Logouts, Content Management and more. But all these standards are in an early stage, most in implementer's draft status. The support is not very good, and lots of details might still change. None of this is a deal breaker. But when you build a CIAM system, you must know which robust foundations you can rely on, and which areas are a bit more diffuse.

Hype 2: Document Centric Identity Proofing (DCIP)

DCIP is not exactly a new topic. But recent trends promise to redefine what it can do.

In the past, Document Centric Identity Proofing – validating identities based on existing ID cards, passports, driver's licenses etc. – was usually implemented directly into business applications. So, the app which was used to unlock and start the car in a rental scenario, was the same app that validated the driver's license before registration. The approach has one major drawback: Identity data can't be easily re-used by other applications. This is bad for everyone involved: It adds friction for the user, and it causes additional costs for the enterprise – identity proving is expensive and having to run a dedicated solution for each app quickly adds up.

Identity Proofing



Therefore, organizations are trying to integrate DCIP into their CIAM systems, to provide robust identity proofing for all applications. However, the challenge in this scenario is not the implementation – typically, we'll simply integrate an out-of-the-box solution for that. The challenge is to provide the data to other applications, as there are multiple different approaches to validate documents and multiple different documents out there. Is standard identity proofing sufficient for the car rental scenario above? Is it sufficient for opening a banking account? Therefore, designing these solutions has always been quite hard and the reason why organizations often ended up with solutions that didn't really fit.

And this is where it gets exciting. The OpenID Connect Foundation has a dedicated working group specifically tasked with the handling of proofing scenarios – and if all goes according to plan, they will provide detailed specifications and regulate how to share verified data with applications.

The project is called OpenID Connect for Identity Assurance 1.0 (OCIA), and if this kind of use case looms large in your enterprise, then I would highly recommend having a look at it before you start designing and implementing your solution. From what I have seen, OCIA describes very thoroughly which kind of information is required and which can be provided. For example: What are the rules for validation, and which trust framework is used? What was the method for proofing: Was it proofed physically in person? Or just AI-based? Or even a simple unsupervised remote video identification? The approach obviously also tracks the time stamps, dates, and document expirations, making the validation even more secure. Now, bear in mind that this specification is not final yet, either. But the first implementer's draft is out there right now, and I don't expect any major changes to that specification.

Hype 3: Bring Your Own Identity

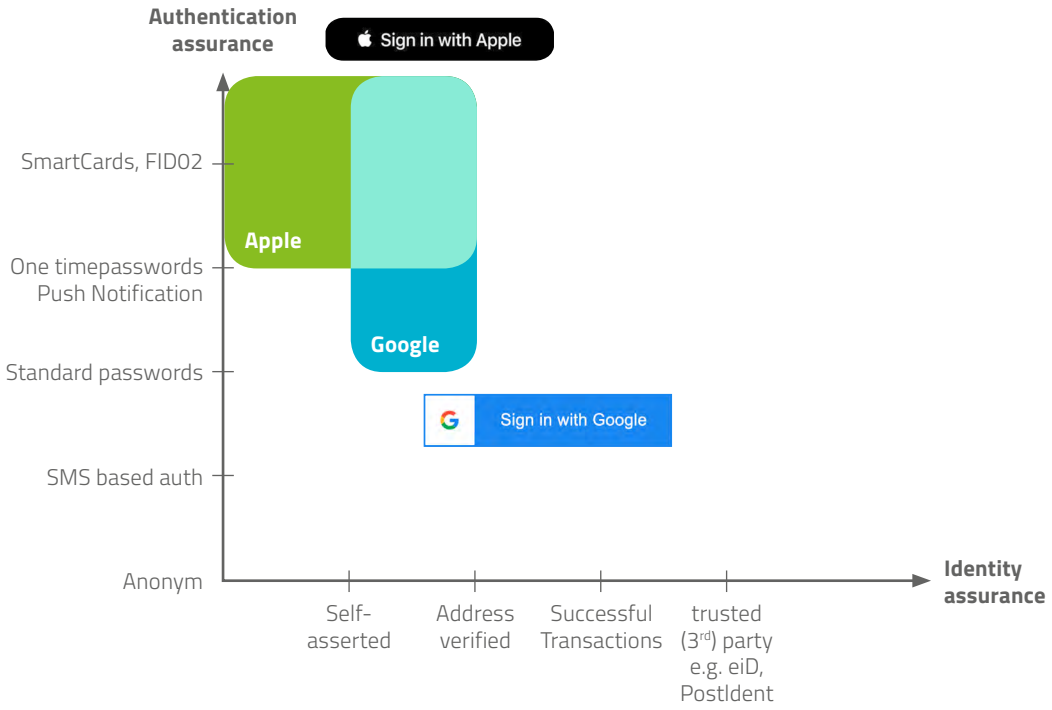
Why Social Login offers more than just a seamless customer experience.

Our next trend is Bring Your Own Identity (BYOI), specifically with regards to identity proofing. So, when we talk about BYOI, we usually mean the login via the Google, Apple, Facebook, or another button – and everyone will agree that this is a very convenient feature. And it's not just convenient, there are multiple other value propositions. But there are also some challenges, so I want to present you a toolbox we use when designing this kind of BYOI journey, and I also want you to understand which level of security this can provide – both looking at authentication assurance and at identity assurance.

Before we delve deeper into the technology, it's paramount to understand that Identity Assurance and Authentication Assurance are two very different dimensions: When we are talking about identity assurance, we are usually looking at self-asserted data: Google never asks the customers to show their ID card. So, they only deliver to you what the customer previously told them. Often, you will later use your customer processes to improve those account details in your CIAM system without ever telling Google. But as far as authentication is concerned, Google is providing a great level of security in this step. Yes, it is password-based authentication, but there are also multiple risk-based capabilities: They will check if a user account has likely been compromised; they will check for new devices; and they are also looking into offering stronger authentication options than just a password. Now unfortunately, you never know which kind of authentication they will end up using, but awareness and willingness are definitely there. Also, please note that Google is just one example. Many other large platforms – Facebook, Meta, Twitter, and Instagram, to name a few – are taking a similar route and are using similar approaches.

One company that deserves a special mention in this context is Apple. Together with Google, Apple is probably the most relevant vendor for the third-party login, as most CIAM use cases are relying on mobile phones and almost everyone is using one of the two platforms. But what's special about Apple is that they are forcing every single user to use strong authentication. Without strong authentication, your users cannot access the Apple capabilities. So, as long as a user is accessing your apps while logged-in with Apple, you can be absolutely certain that they have used strong MFA, and that's a great thing to know.

The less attractive flip side of the coin is that Apple will not always provide the self-asserted data of the customer. Sometimes, they will withhold the name. Sometimes, you will not get a real email address, but a pseudo address generated by Apple instead.



And when that happens, you will always have to contact Apple if you want to contact the user – which you will not always want to do. That said, all of this is up to the user, to your customer: They are the ones who decide to share their email address or to hand over a pseudo address issued by Apple. BYOI has a bright future ahead, and it is a major trend to recon with. That said, there are also some pitfalls.

First off, while it's very easy to implement the happy path, things become much more complicated when looking at fringe cases. What if a user has already registered for your service, and generated a password in your sign-in system – but then decides for whatever reason to login with the Apple or Google button? Will you be able to detect this, and to match these accounts? What if he asks you to link the accounts later? And what if he uses Apple today and Google tomorrow? This is obviously not a scenario which will occur every day, but you must be aware of the possibility. And don't worry – matching accounts in these situations is no rocket science, and many CIAM solutions already support the capability. But if you are not aware of this pitfall, it will result in a poor customer experience, so it's important to keep it in mind.

Another problematic issue is Apple, or more specifically the private relay email address we mentioned earlier, as you have to follow very specific rules if you want to send a mail through Apple. Also, bear in mind that your Apple customers could switch to Google someday, and if you only have their Apple pseudo addresses, it will become much harder to reach out to these users. Once again, this is not a deal breaker for BYOI by any means – but it's another small thing you must be aware of, and a valuable reminder that all these brand-new trends and technologies are still at an early maturity level, so they will require a bit more diligence and attention than your established run-of-the-mill solutions.

Hype 4: MFA and Password-Less Authentication

Is FIDO2 the technology we need to do away with passwords for good?

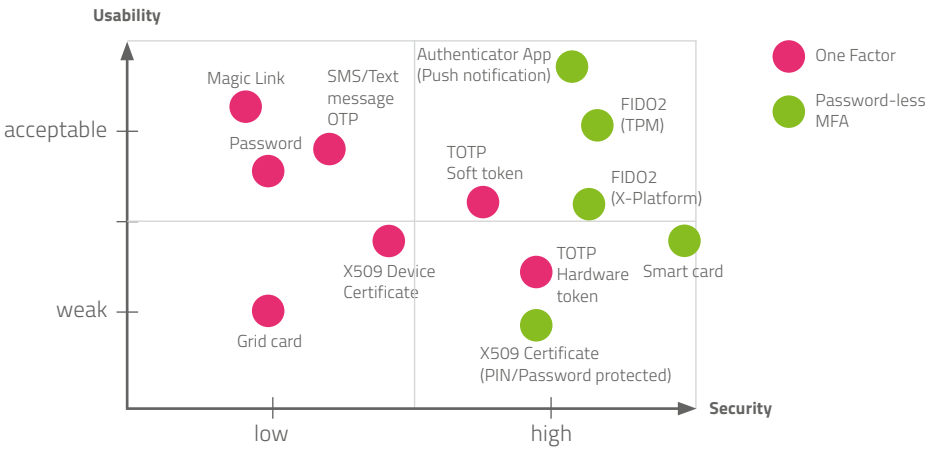
Speaking of Apple, I already mentioned that they are really good at authenticating their customers. Not only will they provide a robust scoring for each user – indicating if it is a real user or a bot, and how likely each of the two is – but they also enforce Multi-Factor Authentication which is very, very valuable. There are many reasons why an organization will want strong MFA in their CIAM system – but the most important one is really simple: Nobody likes passwords, and MFA is a great starting point to do away with passwords altogether. Now, I will be the first one to admit that passwords have one big advantage: Everybody knows how to use them. So, you will never have to train your customers on how to use a password. Unfortunately, their security is very low, and depending on policies to enforce them is just not acceptable anymore.

Thankfully, modern authentication solutions offer a broad set of alternatives. Some of them use a single factor – they might send a text message to a phone or push a notification to an app – while the stronger ones require multiple factors, and an even smaller group is doing this in a password-less way. And this small subset is probably the most exciting part – technologies like mobile apps which generate a one-time password and combine it with the crypto-components of the hardware and the biometric features or the PIN on the phone. These solutions combine a high and adaptive level of security with a great, seamless experience, since everything unfolds on the user's smartphone, and they definitely warrant a closer look.

When looking at password-less authentication, the one authentication protocol which we should be aware of is the FIDO2 protocol. Basically, there are two strands of FIDO2:

The first option is to utilize existing hardware, usually the mobile phone or the notebook; the second is to use a dedicated external token. Now, in most CIAM use cases you won't want to send out hardware tokens to your customers due to scaling effect – this would only make sense in very specific situations in which you have to protect very valuable services. That said, both options are available, and both are user friendly and very secure. If you look into Gartner's analysis of CIAM use cases, they tend to recommend FIDO2, either with hardware tokens or with mobile phones. And I think this is a really robust and future-proof apprwoach, and one which several of our customers have already taken.

Multi-Factor Authentification and Password-less



But once again, FIDO2 also comes with some challenges we need to address. So, FIDO2 is typically about a combination of 'What you know', 'What you have' and a biometric component. In most implementations, it uses the hardware as a token as well as biometrics or a PIN. But while FIDO2 supports a broad ecosystem of platforms – Windows 10 and 11, macOS and Android as well as the Edge, Chrome, and Firefox browsers – and offers the same robust authentication on each of them, the GUI looks completely different on each system. This means that you don't have any influence (or even any idea) what your customer will see when he accesses your service. And what's even worse: If they should use an unsupported browser – like the embedded browsers used by Cisco AnyConnect and other VPN solutions – your authentication might not work at all. Now, as we typically don't provide VPN to customers, this will usually not be a relevant CIAM issue – but once again, you should keep this scenario in mind.

Hype 5: Decentral Identity Management

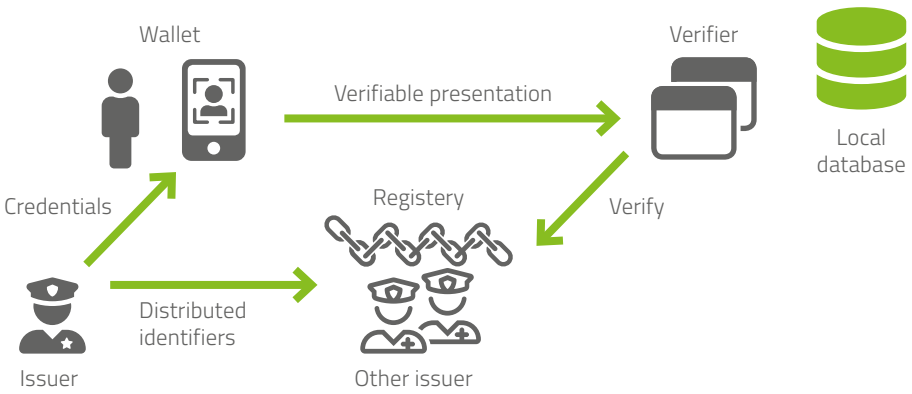
How Blockchain technology could shape the future of CIAM.

And with that, let's have a look at today's final trend: Decentral Identity Management. As you all know, most modern CIAM solutions follow a centralized approach: They use a central repository in which accounts for customers are generated, and the organization itself is in charge of this user repository. But one of the hot topics in CIAM is a decentral management of identities – and as this is a very exciting approach, let's have a look at what this means.

Decentralized Identity Management solutions typically consist of two components:

- The first component is a digital wallet, usually on your customer's phone. It contains his credentials, and as those credentials are usually created by the customer himself, it's his wallet not yours, which is an important distinction.
- The second component is a distributed ledger. This is a blockchain technology – so it's not just your organization providing credentials for each user, but other organizations as well – which are very loosely tied to your organization.

Decentralized Identities



Can you see why this is such an exciting technology? Let's say you issued credentials to the user. Once you validate his identity – maybe with his passport, his driver's

license, or some other information you generated based on your digital services – all his information (his name, his address, his age) is stored on his phone, not in your repository. Then, whenever the user wants to access an application – which might be in any organization – he'll be able to send his verifiable identification to that app. The application will then have a look at what has been sent, by verifying the entry in the "Distributed Ledger" registry and checking if what he sent is indeed stored there. The big thing is that the registry does not contain any clear text information – the verification is based on hashes, on the Distributed Identifier you provided. Once the verifier confirms everything is in order, it will grant access to the user.

Let this idea sink in: The PII claim provided by the user is not shared by your organization, and it's not provided by the registry, the blockchain, but by the user himself. This means that the user remains in full control of his data. There's also no risk of leakage or a data breach, as everything relevant is only stored on his phone.

That's both a good thing and a bad thing. Let's look at the advantages first:
For the user, the most exciting part will be that any claims provided can be reused for multiple organizations – so there's no need to provide a dedicated Identifier for each organization whose digital services the customer wants to access. That's a huge benefit. Another thing which is really awesome, even if these solutions are still at an early stage, is the user experience: Since the app, the mobile app and the wallet are all located on the same device, there are no browser windows opening, no redirections and no data entries – that's quick, easy and very usable.

Also, as everything is happening on the phone, the customer communication promises to be very seamless. The idea of reusing already verified, approved data offers a great experience which the users will appreciate: No one likes identity proofing scenarios where they must hold their ID card in front of the camera in the right angle.

And then, there are the security aspects. One big plus is that this is a fully password-less approach, where the wallet is protected on the phone. So, there's no risk of password data breaches. Another benefit is that the privacy is very good, too, as the user is always in control of the wallet and decides himself, which application will have access to which information.

But of course, there are some drawbacks we need to talk about as well. One is that if you are asking your customers for personal information – maybe an age confirmation you need for the business applications you are offering –, chances are you will need that data in the future as well. So, you will probably want to store it. And therefore, you will still need provisioning capabilities and consent management capabilities to a certain degree, so the distributed identity will not solve all challenges for you.

Also, everything we said about tokens applies here as well – you will need the same tools you would when leveraging distributed identities. And it's important to bear in mind that the standards we see are not quite mature yet. While there are some implementations out there, they are usually not yet in real world scenarios. This is a very new technology, and all the usual cautions apply, maybe even more so, since a wallet is so important: Therefore, we must not take any risks, and we need to take any challenges very seriously. But even if a lot of improvement is still needed, I fully expect that a few years down the road, Google, Apple, and all major mobile operating systems will support wallet capabilities – maybe based on what the OpenID Connect working group is working on, maybe based on other standards.

Conclusion

In our increasingly digital business world, a strong Customer Identity and Access Management is becoming more and more relevant. Customer demands are growing: Your users expect you to deliver a seamless experience, while offering strong security and protecting their personal data – and if you fail to deliver on the promise, they might very well abandon your brand altogether. The good news is that today's powerful new CIAM technologies will go a long way in accommodating your customers' wishes – and tomorrow's trends promise even more exciting capabilities. iC Consult can help you evaluate the different technologies and unlock their full potential for your organization.

About iC Consult

iC Consult is the world's leading independent consultancy, systems integrator, and managed services provider for Identity & Access Management with more than 800 employees worldwide.

We are committed to excellence and innovation, and with the best-in-class technology in the IAM space, we provide our customers with next-level cybersecurity solutions. Our service portfolio covers Managed Services for IAM including advisory, architecture, implementation, integration, support, and operations.

iC Consult is headquartered in Germany with offices in Switzerland, Austria, France, Belgium, Spain, Bulgaria, the UK, the U.S., Canada, India, and China. The world's largest brands trust in our expertise, to secure and manage their most valuable assets: their identities.

More information at www.ic-consult.com